IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**CRIMINAL NO. 21-203**
TERRELL ASHBY **a/k/a "Jason Brandon"**	**:**	

GOVERNMENT'S CHANGE OF PLEA MEMORANDUM

I. INTRODUCTION

Defendant Terrell Ashby has informed the government that he wishes to plead guilty to all counts in the Indictment, charging him as follows:

- Count One: cyberstalking resulting in serious bodily injury, in violation of 18 U.S.C. §§ 2261A(2)(B) and 2261(b)(3);
- Count Two: extortion, in violation of 18 U.S.C. § 875(d);
- Count Three: cyberstalking, in violation of 18 U.S.C. § 2261A(2)(B); and
- Count Four: extortion, in violation of 18 U.S.C. § 875(d).

These charges arise from the defendant's sextortion scheme, in which he solicited explicit images and videos of women online based on fraudulent promises, and then used those images to extort the women by threatening to release the images and videos unless he was paid.

II. PLEA AGREEMENT

There is no plea agreement in this case; the defendant is pleading open to the indictment.

III. MAXIMUM PENALTIES

The Court may impose the following maximum sentences: on Count One (cyberstalking resulting in serious bodily injury), 10 years' imprisonment, a three-year period of supervised

release, a $250,000 fine, and a $100 special assessment; on Count Three (cyberstalking), 5 years' imprisonment, a three-year period of supervised release, a $250,000 fine, and a $100 special assessment; and on each of Counts Two and Four (extortion), two years' imprisonment, a one-year period of supervised release, a $250,000 fine and a $100 special assessment. Thus, the total maximum sentence is: 19 years' imprisonment, 10 years of supervised release, a $1,000,000 fine and a $400 special assessment. Full restitution of at least $28,883.64 shall be ordered. Forfeiture of all proceeds from the offense also may be ordered. Further, the defendant's supervised release may be revoked if its terms and conditions are violated, in which case the original term of imprisonment may be increased by up to two years on Counts One and Three and by up to one year on Counts Two and Four.

VI. ELEMENTS OF THE OFFENSE

A. Count One (cyberstalking resulting in serious bodily injury)

In order to prove that the defendant violated 18 U.S.C. §§ 2661A(2) and 2261(b)(3), the government must prove beyond a reasonable doubt that the defendant:

1. With the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person;

2. Used the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that

3. Caused, attempted to cause, or would be reasonably expected to cause substantial emotional distress to that person, an immediate family member, or a spouse or intimate partner; and

4. The offense resulted in serious bodily injury to the victim.

"Serious bodily injury" is defined as "bodily injury which involves…a substantial risk of death." 18 U.S.C. § 1365(h)(3) (which is referenced in §§ 2266(6) and 2119(2) as the appropriate definition).

B. Count Three (cyberstalking)

In order to prove that the defendant violated 18 U.S.C. §§ 2661A(2), the government must prove beyond a reasonable doubt that the defendant:

1. With the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person;

2. Used the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that

3. Caused, attempted to cause, or would be reasonably expected to cause substantial emotional distress to that person, an immediate family member, or a spouse or intimate partner.

C. Counts Two and Four (extortion)

In order to prove that the defendant violated 18 U.S.C. § 875(d), the government must prove beyond a reasonable doubt that:

1. The Defendant knowingly sent a message in interstate/foreign commerce containing a true threat to damage the reputation of another; and

2. The Defendant did so with the intent to extort money or something else of value to the Defendant.

V. FACTUAL BASIS FOR THE PLEA

If this case were to go to trial, the government would prove each element of the charged offenses beyond a reasonable doubt by introducing witness testimony, digital and forensic evidence, financial records, records from cellular and internet service providers and items seized during the search of the defendant's residence.

The evidence would show that, from at least February 2020 through mid-December 2020, Ashby engaged in a pattern of online solicitation, exploitation, and extortion by fraudulently obtaining explicit videos and photos of women and then threatening their release unless he was

paid. In furtherance of this scheme, Ashby created numerous profiles on social media platforms Instagram and Snapchat, all under the false identity of "Jason Brandon" (using variations on that name). Using Instagram, Ashby sent online Direct Messages (DMs) to **hundreds** of women offering to pay them $70,000. When he received a response indicating interest in his offer, he would ask the victim to provide her Snapchat, PayPal, and/or Cash App usernames so that he could send the money he promised. In an attempt to appear legitimate, he used a profile photo depicting large amounts of cash bound with currency straps. He also often sent his victims altered screenshots of online money transfers he purportedly sent to other women.

Ashby transitioned the women from Instagram to Snapchat, a social media platform with a reputation as being more "secure" in that shared photos and videos are not generally saved unless specific actions are taken by a user, which results in immediate notification to the other party (e.g., "John Doe took a screenshot"). Ashby convinced his victims to conduct video chats while nude and/or send him explicit photos, all with the promise of sending them money in return. Ashby directed the women what to do, including posing in specific ways. Although the women provided video and audio during these interactions, Ashby only sent messages through the chat feature on Snapchat and never enabled his camera or microphone, thereby concealing his true identity. Indeed, Ashby kept a piece of black tape over the camera lens of his Apple iPhone to ensure his identity would not otherwise be accidentally disclosed while engaging with his victims.

Ashby took screenshots during these video chats, capturing explicit images of the women without their knowledge. Then he extorted the women, threatening that he would disseminate these images unless they paid him. Many women succumbed and paid Ashby anywhere from $25 to $50 using online payment platforms PayPal and Cash App. Ashby linked these online

accounts to his Langley Federal Credit Union bank account, and subsequently transferred his victims' money to his own account and withdrew the funds. Records from CashApp and PayPal show that, between April 7, 2020 and December 18, 2020, Ashby received over $23,000 in transfers. Records from Ashby's federal credit union show that, during that same time frame, he received approximately $24,173 into his account and withdrew the same amount in cash. During a search of Ashby's residence, agents found approximately $25K in cash bound in currency straps (consistent with his online profile pics) in the top dresser drawer in Ashby's bedroom.

Ashby also created numerous shaming profiles on Instagram and Snapchat using his victims' identities and explicit photos. He messaged his victims, threatening that their "expose" page had been created, and also messaged many of his victims' legitimate social media followers and friends advertising these "expose" pages. In some cases, Ashby used random cell phone numbers in order to send harassing text messages to victims whose cell phone numbers he had obtained. Ashby often threatened that he would only stop once his victims paid what he believed he was owed. In some instances, Ashby continued to send these threats after the initial extortion, even when the victims had paid him.

VICTIM 1

With regard to Victim 1 (the basis for Counts One and Two), on August 21, 2020, at approximately 1:02 AM, Ashby used Instagram profile "jbrand0n.1993" to send a solicitation message to Victim 1, a 20 year-old woman residing in Newtown Square, Pennsylvania. Ashby offered Victim 1 a large sum of money if she agreed to participate in a nude video chat with him on Snapchat. Victim 1 agreed and engaged in a nude video chat with Ashby, who was using the Snapchat profile "Jasonbrandon199."

During the video chat, which occurred during the early morning hours of August 22, 2020, Ashby surreptitiously captured several explicit screenshots of Victim 1 without her consent. Ashby then sent Victim 1 multiple messages demanding that she pay him $40 to delete the nude photos or he would expose her. Specifically, Ashby wrote, in part, "[w]hen you send the $40 I will delete your nudes offline" and "Just send the $40 and you're good lol[.] We aren't good until you send the $40[,] simply send the $40 and I'll delete it[.]" Victim 1 then paid Ashby $40 by transferring money to his Cash App profile "slispopas4." That same day, Ashby transferred this money from Cash App to his Langley Federal Credit Union bank account.

Despite the $40 payment, Ashby continued to demand more money from Victim 1, threatening to send the nude images to her college and other social media friends if she didn't pay him. For example, Ashby wrote, in part:

> Your expose page is being created right now and I'm also going to tag your college[.] I'll end you[.] I'm not someone you want to [expletive] with[,] go tell your father that
> …
> Just [sent] your nudes to [name redacted]
> Already exposed you whore
> Your life is over
> You're dumb if you thought this was over its not over until my $134 is sent
> I'll make sure our whole school sees your nudes

As a result of the continued extortion, Victim 1 became distraught and ingested a number of prescription pills in an attempt to calm her emotional distress. She was rushed to an emergency room in an ambulance and ultimately recovered.

While Victim 1 was hospitalized, on August 22, 2020, Ashby began advertising the nude photos of Victim 1 using various accounts on both Instagram and Snapchat. On September 1, 2020, Ashby again advertised Victim 1's nude photos by creating another new account on Snapchat. On November 1, 2020, Victim 1 received another extortionate message from Ashby,

who was using a new Instagram account with the name "jbrandon1993_3." The extortionate message read as follows:

> Remember those pics you sent me and I posted and that facetime I screenrecorded? I'm not stopping until you send what you owe[.] I DM'd 50 people you follow the pics you sent me[.]

VICTIM 2

With regard to Victim 2 (the basis for Counts Three and Four), on June 28, 2020, Ashby used Instagram profile "jasonbrandon199" to send an initial solicitation message to Victim 2, a 21 year-old woman residing in West Chester, Pennsylvania. Ashby offered to send $70,000 to Victim 2 and the conversation transitioned to Snapchat.

Once on Snapchat, Ashby used profile "Jasonbrandon199" to solicit nude photographs of Victim 2, promising to send her money in return. Ashby told Victim 2 how to pose in the "snaps" (i.e., photos) she sent, directing her to use a mirror and sit on her feet with her backside facing the camera. She initially attempted to hide her face, but Ashby was insistent that her face be included and she ultimately relented. Victim 2 provided 8 "Snaps" to Ashby, some partially nude and some fully nude. Unbeknownst to Victim 2, Ashby took screenshots of the nude Snaps.

Ashby then began extorting Victim 2 over the threatened release of the photos and directed her to transfer money to him at PayPal account "qrichards377@gmail.com." Victim 2 sent one payment in the amount of $25 to Ashby at 7:17 PM (EDT), and subsequently blocked him when he began demanding more money.

Ashby then created a new Instagram profile ("[Victim 2]nudes") on June 28 and two new Snapchat profiles ("zeta[Victim 2]nud20") & "[Victim 2]urfucked") on June 30 and sent Victim 2 friend requests/invitations to connect with the intent of harassing and shaming her.

Respectfully submitted,

JACQUELINE C. ROMERO
United States Attorney

/s/ Sarah M. Wolfe
SARAH M. WOLFE
Assistant United States Attorney

Dated: April 17, 2024

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Government's Change of Plea Memorandum has been served by e-mail upon the following:

Michael McCrossen, Esquire
601 Walnut Street, Suite 540W
Philadelphia, PA 19106
Catherine_henry@fd.org

/s/ Sarah M. Wolfe
SARAH M. WOLFE
Assistant United States Attorney

DATED: April 17, 2024